Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée

Table des matières

Introduction

Ce document décrit les étapes pour contourner le trafic des mises à jour Microsoft dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.

Cisco recommande d'installer les outils suivants :

- SWA physique ou virtuel
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Mises à jour Microsoft

Les mises à jour Microsoft sont des correctifs essentiels, des mises à jour de sécurité et des améliorations de fonctionnalités disponibles par Microsoft pour ses systèmes d'exploitation et ses applications logicielles. Ces mises à jour sont essentielles au maintien de la sécurité, de la stabilité et des performances des ordinateurs et des périphériques réseau. Ils garantissent que les systèmes sont protégés contre les vulnérabilités, que les bogues sont corrigés et que de nouvelles fonctionnalités ou améliorations sont intégrées dans le logiciel.

L'impact des mises à jour Microsoft sur les serveurs proxy, tels que Cisco SWA, peut être important. Ces mises à jour impliquent souvent le téléchargement de fichiers volumineux ou de nombreux fichiers plus petits, ce qui peut consommer une bande passante et des ressources de traitement considérables sur le proxy. Cela peut entraîner un encombrement, des performances réseau plus lentes et une charge accrue sur l'infrastructure proxy, ce qui peut affecter l'expérience utilisateur globale et d'autres opérations réseau critiques.

Le contournement du trafic Microsoft Update à partir du proxy peut être un moyen sûr et efficace de gérer ces défis. Étant donné que les mises à jour Microsoft proviennent de serveurs Microsoft approuvés, permettre à ce trafic de contourner le proxy peut aider à réduire la charge sur le serveur proxy sans compromettre la sécurité du réseau. Cela garantit que les mises à jour essentielles sont fournies efficacement tout en préservant les ressources proxy pour d'autres tâches de sécurité et de filtrage de contenu. Cependant, il est important de mettre en oeuvre ces configurations de contournement avec soin afin de maintenir la sécurité globale du réseau et la conformité avec les politiques de l'entreprise.

Ignorer les mises à jour Microsoft

Si vous envisagez d'éviter le trafic des mises à jour Microsoft par proxy, il existe deux approches principales

1. Contournement : cela implique de configurer le réseau pour rediriger le trafic afin qu'il n'atteigne jamais le SWA.
2. Passthrough : cela implique de configurer le SWA pour ne pas décrypter ni analyser le trafic des mises à jour Microsoft, lui permettant de passer par le proxy sans inspection.

Contournement du trafic dans SWA

Pour contourner le trafic des mises à jour Microsoft sur les réseaux équipés de SWA, l'approche varie en fonction de la configuration de votre déploiement de proxy :

Type de déploiement	Contournement du trafic
Déploiement transparent	Vous pouvez rediriger le trafic des mises à jour Microsoft au niveau du routeur ou des commutateurs de couche 4 qui sont responsables du transfert du trafic vers le serveur

	proxy.
	Vous pouvez configurer les paramètres de contournement directement dans l'interface utilisateur graphique (GUI) de SWA.
Déploiement explicite	Pour empêcher le trafic des mises à jour Microsoft d'atteindre le SWA, vous devez configurer le contournement à la source. Cela signifie qu'il faut exempter les URL pertinentes sur les ordinateurs clients pour s'assurer que le trafic n'est pas redirigé vers le SWA.

Si le contournement d'un trafic spécifique nécessite une reconception complète du réseau et n'est pas réalisable, une autre approche consiste à configurer le SWA pour qu'il passe par certains types de trafic. Cela peut être réalisé en configurant le SWA pour ne pas décrypter ni analyser le trafic désigné, lui permettant de passer par le proxy sans inspection. Cette méthode garantit que le trafic essentiel est acheminé efficacement tout en minimisant l'impact sur les performances du réseau et les ressources proxy.

Étapes de transmission des mises à jour Microsoft

Les trafics Passthrough Microsoft Updates se décomposent en quatre étapes principales :

Étape	Étapes
1. Créer une catégorie d'URL personnalisée pour les URL de mises à jour Microsoft	Étape 1.Dans l'interface utilisateur graphique, sélectionnez Gestionnaire de sécurité Web, puis cliquez sur Catégories d'URL personnalisées et externes. Étape 2.Cliquez sur Ajouter une catégorie pour ajouter une catégorie d'URL personnalisée. Étape 4.Attribuez un nom de catégorie unique. Étape 5. (Facultatif) Ajoutez une description. Étape 6. Dans Ordre de la liste, choisissez la première catégorie sur laquelle vous voulez vous positionner. Étape 7. Dans la liste déroulante Type de catégorie, sélectionnez Catégorie personnalisée locale. Étape 8. Ajoutez des URL de mises à jour Microsoft dans la section Sites.

	Conseil : vous pouvez consulter la liste des mises à jour Microsoft à partir de ce lien : [Étape 2 - Configurez WSUS | Microsoft Learn] Attention : ne copiez/collez pas les URL telles qu'elles sont dans les documents Microsoft ; formatez-les correctement au format SWA. Pour plus d'informations, consultez : [Configurer des

	[catégories d'URL personnalisées dans Appareil Web sécurisé - Cisco] Étape 9. Envoyer.
2. Créez un profil d'identification pour exempter le trafic des mises à jour Microsoft de l'authentification	Étape 10.Dans l'interface utilisateur graphique, sélectionnez Gestionnaire de sécurité Web, puis cliquez sur Profils d'identification. Étape 11.Cliquez sur Ajouter un profil pour ajouter un profil. Étape 12.Utilisez la case à cocher Activer le profil d'identification pour activer ce profil ou le désactiver rapidement sans le supprimer. Étape 13.Attribuez un profileName unique. Étape 14. (Facultatif) Ajoutez une description. Étape 15. Dans la liste déroulante Insérer ci-dessus, choisissez l'emplacement de ce profil dans le tableau. Étape 16. Dans la section Méthode d'identification de l'utilisateur, sélectionnez Exempter de l'authentification/identification. Étape 17.Dans la section Define Members by Subnet (Définir les membres par sous-réseau), si vous souhaitez transmettre le trafic Microsoft à certains utilisateurs spécifiques, entrez les adresses IP ou les sous-réseaux qui s'appliquent, ou laissez ce champ vide pour inclure toutes les adresses IP. Étape 18. Dans la section Avancé, sélectionnez Catégories d'URL personnalisées. Étape 19. Ajoutez la catégorie d'URL personnalisée qui a été créée pour les mises à jour Microsoft. Étape 20. Cliquez sur Done. Étape 21. Envoyer.
3. Créer une stratégie de déchiffrement pour transmettre le trafic des mises à jour Microsoft	Étape 22.Dans l'interface utilisateur graphique, sélectionnez Gestionnaire de sécurité Web, puis cliquez surStratégie de décodage. Étape 23. Cliquez sur Ajouter une stratégie pour ajouter une stratégie de décodage.

	Étape 24. Cochez la case Activer la stratégie pour activer cette stratégie. Étape 25.Attribuez un PolicyName unique. Étape 26. (Facultatif) Ajoutez une description. Étape 27.Dans la liste déroulante Insérer la stratégie ci-dessus, sélectionnez la première stratégie. Étape 28.Dans lesProfils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé dans les étapes précédentes. Étape 29. Envoyer. Étape 30.Dans la page Politiques de déchiffrage, sous Filtrage des URL, cliquez sur le lien associé à cette nouvelle politique de déchiffrage. Étape 32.SélectionnezPassthrough comme action pour la catégorie d'URL Mises à jour Microsoft. Étape 32. Envoyer.
4. Créer une stratégie d'accès pour autoriser le trafic des mises à jour Microsoft	Étape 33.Dans l'interface utilisateur graphique, sélectionnez Gestionnaire de sécurité Web, puis cliquez sur Stratégie d'accès. Étape 34. Cliquez sur Ajouter une stratégie pour ajouter une stratégie d'accès. Étape 35. Cochez la case Activer la stratégie pour activer cette stratégie. Étape 36.Attribuez un PolicyName unique. Étape 37. (Facultatif) Ajoutez une description. Étape 38.Dans la liste déroulante Insérer au-dessus de la stratégie, sélectionnez la première stratégie. Étape 39.Dans la liste Profils d'identification et utilisateurs, sélectionnez le profil d'identification que vous avez créé dans les étapes précédentes. Étape 40. Envoyer. Étape 9. Sur la page Access Policies, sous URL Filtering, cliquez sur le lien associé à cette nouvelle stratégie d'accès Étape 10.Sélectionnez Autoriser l'action pour la catégorie d'URL personnalisée créée pour les mises à jour Microsoft.

	Étape 11. Envoyer. Étape 12. Valider les modifications.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - GD(General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance] - Cisco
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Comment exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web Cisco (WSA) - Cisco
- Utilisation des meilleures pratiques d'appliance Web sécurisé - Cisco
- Contourner l'authentification dans l'appareil Web sécurisé - Cisco

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.